IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE **ORAL ARGUMENT REQUESTED**

MEMORANDUM OF LAW IN SUPPORT OF
DEFENDANTS' MOTION TO DISMISS THE AMENDED COMPLAINT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Regulations

Other Authorities

PRELIMINARY STATEMENT

In December 2020, SolarWinds learned it had suffered an extraordinarily sophisticated cyberattack by the Russian government. It responded just as a public company should, by promptly and transparently disclosing the incident. Nonetheless, more than three years later, the SEC seeks to invent a basis for an enforcement action where there is none, bringing securities fraud and controls charges against SolarWinds and its current Chief Information Security Officer ("CISO"), Tim Brown. The charges are as unfounded as they are unprecedented. The SEC is trying to expand cybersecurity disclosure obligations well beyond what the law requires, and, with the controls charges, claim a mandate for substantively regulating cybersecurity that the agency does not have. The case is fundamentally flawed and should be dismissed in its entirety.

As reflected by the SEC's long and rambling Amended Complaint, this is a case in search of a theory: The SEC has thrown everything it can think of against the wall, but nothing sticks. The SEC tries to allege fraud based on SolarWinds' statements to investors—including its risk disclosures before the attack and the 8-K filed once the attack was discovered—but it cannot plausibly claim either was misleading. The risk disclosures specifically warned that SolarWinds' systems "are vulnerable" to "sophisticated nation-state" actors—the very risk that materialized. The SEC contends the disclosures should have included detailed information about the Company's vulnerabilities, but that is not the law, for good reason: publishing such details would be unhelpful to investors, impractical for companies, and harmful to both, by providing roadmaps for attackers. As for the 8-K, it disclosed the key facts about the attack and the material risks it presented, including that as many as 18,000 customers were at risk of compromise. Given these candid disclosures, the SEC's contention that SolarWinds hid the seriousness of the attack is baseless.

Scrambling to find something—*anything*—to justify its securities fraud charges, the SEC resorts to challenging statements that SolarWinds made not to the investing public but *to customers*

on its website. According to the SEC, shortly after being hired in July 2017 as Vice President of Security Architecture, Mr. Brown concluded that SolarWinds had "poor" cybersecurity and sought to hide this from investors—never mind that the Company had no public investors at the time, as its IPO was more than a year away—by publishing a page on the Company's website telling customers about its cybersecurity policies (the "Security Statement"). Mr. Brown is alleged to have devised this "scheme" on his own and to have maintained it for years—despite not even having an executive position at the time and having nothing to gain from lying—all in order to deceive investors, to whom the Security Statement was never even mentioned. Notably, even though it had three years of investigation to get its facts straight, the SEC made no mention of Mr. Brown hatching any such "scheme" in its original Complaint, but only thought to add these allegations now in an attempt to find some theory to hold its case together.

It doesn't work. The alleged "scheme" is implausible on its face and is unsupported by any well-pled facts suggesting Mr. Brown ever acted with any intent to deceive or conscious disregard for the truth. Despite collecting countless documents, the SEC cannot point to a single one discussing the purported years-long scheme; and despite taking the testimony of numerous witnesses, the SEC cannot point to a single one who ever accused Mr. Brown—or anyone at the Company—of such misconduct. Instead, the SEC simply alleges SolarWinds had various security deficiencies, and then speculates that Mr. Brown perpetrated some sort of cover-up. That is hardly enough to satisfy its pleading burden. Moreover, the starting premise of the SEC's theory—that SolarWinds failed to implement certain policies in the Security Statement—is contradicted by the very documents on which the Amended Complaint relies. Those documents make clear that SolarWinds did exactly the things the SEC says it did not do. The SEC repeatedly ignores these contravening facts in the documents, while cherry-picking other snippets that it takes out of

context. When the SEC's mischaracterizations of the documents are corrected, it is clear there is no "scheme" to conceal cybersecurity failures plausibly alleged here. The only party in this case that has made misleading statements about SolarWinds' cybersecurity practices is the SEC itself.[1]

Beyond its fraud claims, the SEC's disclosure controls and internal accounting controls charges also do not pass muster. Even with a second bite at the apple, the SEC fails to identify any disclosure controls that were unreasonably designed. Instead, it merely criticizes the application of those controls, essentially by alleging that SolarWinds and Mr. Brown should have recognized the attack on the Company earlier than they did—a hindsight-driven allegation that could not ground a disclosure controls violation even if it were adequately supported, which it is not. As for the SEC's theory of "internal accounting controls" violations, it amounts to a wholesale rewriting of the law. The agency is trying to twist the concept of *accounting* controls into a sweeping mandate for it to regulate public companies' *cybersecurity* controls—a role for which the SEC lacks congressional authorization or substantive expertise.

For all these reasons, as detailed below, the case should be dismissed—and given that the SEC has already had a chance to amend, and used it liberally, dismissal should be with prejudice.

BACKGROUND[2]

The key facts for purposes of this motion are straightforward: SolarWinds warned investors at all times that its systems were vulnerable to cyberattack. In December 2020, SolarWinds learned

[1] The SEC's misrepresentation of the facts unfortunately fits a pattern of recent conduct by the agency. *See SEC v. Digital Licensing Inc.*, 2024 WL 1157832, at *28 (D. Utah Mar. 18, 2024) (sanctioning the SEC for misrepresenting facts in its complaint and briefing: "Each piece of support the Commission offered … and then later reiterated … proved to be some combination of false, mischaracterized, and misleading.").

[2] Except where noted, all facts stated herein are from the Amended Complaint, cites to which are styled as "¶ [#]." Any exhibits cited are attached to the Declaration of Serrin Turner, and include "documents incorporated into the complaint by reference, legally required public disclosure documents filed with the SEC, and documents possessed by or known to the plaintiff and upon which it relied in bringing the suit," *ATSI Commc'ns, Inc. v. Shaar Fund, Ltd.*, 493 F.3d 87, 98 (2d Cir. 2007), or "matters of which judicial notice may be taken," *Leonard F. v. Israel Discount Bank of N.Y.*, 199 F.3d 99, 107 (2d Cir. 1999).

it had suffered such an attack, which it promptly disclosed, identifying the outer universe of customers at risk. Yet the SEC now alleges that, despite these disclosures, the Company sought to hide its vulnerability to attack and, later, the seriousness of the attack that occurred.

A. SolarWinds Repeatedly Warned Investors It Was Vulnerable to Cyberattack

SolarWinds is a developer of network monitoring software, which many businesses and government agencies use to manage their computer networks. ¶ 43. SolarWinds has (and had during the relevant timeframe) more than 300,000 customers, including nearly all the companies making up the Fortune 500. *Id*. One of its products is the Orion Platform, which consists of a suite of products used for network management. ¶ 44.

Like any technology-focused business, SolarWinds is vulnerable to the pervasive risk of cybersecurity attacks. Thus, when SolarWinds went public in October 2018, it disclosed this risk to investors in its Form S-1 registration statement, along with the material consequences that could follow if an attack succeeded. The disclosure stated in relevant part:

> Our systems and those of our third-party service providers are vulnerable to damage and disruption from ... traditional computer "hackers," malicious code (such as viruses and worms), employee theft or misuse, and denial-of-service attacks, as well as sophisticated nation-state and nation-state-supported actors (including advanced persistent threat intrusions). ... Despite our security measures, unauthorized access to, or security breaches of, our software or systems could result in the loss, compromise or corruption of data, loss of business, severe reputational damage adversely affecting customer or investor confidence, regulatory investigations and orders, litigation, indemnity obligations, damages for contract breach, penalties for violation of applicable laws or regulations, significant costs for remediation and other liabilities.

¶ 240; Ex. 1 at 2–3. SolarWinds noted the risk of a security breach had "increased," as "intrusions around the world have increased" in terms of their "number, intensity and sophistication." ¶ 240.

SolarWinds also disclosed the specific risk of a sophisticated, prolonged attack that could impact its customers. "Because the techniques used to obtain unauthorized access or to sabotage systems change frequently," the Company explained, it "may be unable to anticipate these

techniques or to implement adequate preventative measures," and it "may also experience security breaches that may remain undetected for an extended period." *Id.* Such "security problems," the Company warned, could cause damage not only to its own systems, but also to "our customers' IT infrastructure or the loss or theft of our customers' proprietary or other sensitive information." *Id.* SolarWinds consistently reiterated these warnings or incorporated them by reference in each of its quarterly and annual reports thereafter. ¶¶ 38, 251.

B. SolarWinds Discovered and Promptly Disclosed the SUNBURST Attack

On Saturday, December 12, 2020, SolarWinds learned it had been the victim of a cyberattack: A customer (a leading cybersecurity firm) informed the Company that it had located malicious code in the Orion product, which had evidently been inserted by a threat actor. ¶ 306. This malware—dubbed "SUNBURST"—provided a "backdoor" that the threat actor could use to infiltrate the "network environments of SolarWinds' customers who downloaded and installed the infected versions of the software to systems that were connected to the internet." ¶ 258. The threat actor had inserted the backdoor into three different Orion software versions or "builds," which nearly 18,000 customers downloaded. *Id*. While unknown to SolarWinds when it learned of the incident, the threat actor used the backdoor to conduct attacks on roughly 100 of these customers. *Id.* The federal government concluded that Russia was the threat actor behind SUNBURST, and that the incident was "one of the most ... sophisticated hacking campaigns ever conducted against the federal government and private sector." U.S. GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents* ("GAO Report"), GAO-22-104746, at 1, 14 (Jan. 2022), https://www.gao.gov/assets/gao-22-104746.pdf.

Upon learning of SUNBURST, SolarWinds immediately engaged an outside cybersecurity firm to help investigate and prepared an 8-K to inform the market of the situation. ¶¶ 308, 311. On Monday, December 14—the next trading day—SolarWinds filed a detailed 8-K, explaining:

> SolarWinds Corporation ("SolarWinds" or the "Company") has been made aware of a cyberattack that inserted a vulnerability within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run. SolarWinds has been advised that this incident was likely the result of a highly sophisticated, targeted and manual supply chain attack by an outside nation state, but SolarWinds has not independently verified the identity of the attacker. SolarWinds has retained third-party cybersecurity experts to assist in an investigation of these matters, including whether a vulnerability in the Orion monitoring products was exploited as a point of any infiltration of any customer systems, and in the development of appropriate mitigation and remediation plans. SolarWinds is cooperating with the Federal Bureau of Investigation, the U.S. intelligence community, and other government agencies in investigations related to this incident.

Ex. 2 at 3. The 8-K further explained that up to 18,000 customers had downloaded infected versions of Orion, and that Orion accounted for nearly half the Company's revenue. *Id.* It also noted "significant media coverage of attacks on U.S. governmental agencies and other companies, with many of those reports attributing those attacks to a vulnerability in the Orion products." *Id.* SolarWinds stressed that its investigation was "preliminary and on-going" but identified "numerous financial, legal, reputational and other risks to SolarWinds" from the attack. *Id.* at 5. SolarWinds' stock price dropped nearly 25 percent over the next two days, ¶ 20, indicating investors well understood the severity of the situation.

SolarWinds repeatedly updated investors about the incident, including in Forms 8-K filed on December 17, 2020, Ex. 3, and January 11, 2021, Ex. 4. The January 8-K provided a detailed timeline of the attack and explained the Company's ongoing coordination with "law enforcement, the intelligence community, governments and industry colleagues." *Id.* at 5. The Company also disclosed that, as part of its investigation, it was "reviewing historical and current customer inquiries," and had "identified two previous customer support incidents that, with the benefit of hindsight, we believe may be related to SUNBURST," noting it had been unable to identify the root cause of the reports at the time they were made. *Id.* As the SEC stated at the initial case conference, this January 8-K marks the end of what the Complaint defines as the "Relevant

Period," which extends from the Company's IPO in October 2018 to January 12, 2021, the day after this 8-K was filed. ¶ 1; Hr'g Tr. 4:21–5:8, Dec. 14, 2023, ECF No. 32.

C. After Nearly Three Years of Investigation, the SEC Brings This Lawsuit

While other federal agencies worked cooperatively with SolarWinds in investigating SUNBURST and mitigating the impacts of this nation-state attack, the SEC instead fixated on finding targets to charge with securities violations. It not only investigated SolarWinds (for nearly three years), but also requested, under threat of enforcement, information from many of SolarWinds' *customers*, and questioned *their* disclosures.[3] The SEC has never before litigated an action in federal court against any public company over its cybersecurity disclosures or brought internal accounting controls violations based on alleged deficiencies in cybersecurity controls with no nexus to accounting. Nor has it ever individually charged a CISO.

The SEC filed its original, 68-page Complaint in this matter on October 30, 2023. ECF No. 1. After Defendants moved to dismiss, supported by numerous *amici* explaining the harmful cybersecurity ramifications of the SEC's positions, the SEC responded by doubling down, filing an Amended Complaint ("AC") weighing in at 112 pages. Like the original Complaint, the AC brings claims for fraud and false statements (under Securities Act § 17(a), Exchange Act §§ 10(b) & 13(a), and Rule 10b–5), disclosure controls violations (under Rule 13a–15(a)), and internal accounting controls violations (under Exchange Act § 13(b)(2)(B)), against both the Company and Mr. Brown, along with aiding-and-abetting charges against Mr. Brown. ¶¶ 332-66.

[3] *See* Christopher Bing et al., *Wide-ranging SolarWinds Probe Sparks Fear in Corporate America*, Reuters (Sept. 10, 2021), https://www.reuters.com/technology/exclusive-wide-ranging-solarwinds-probe-sparksfear-corporate-america-2021-09-10; SEC, *In the Matter of Certain Cybersecurity-Related Events (HO-14225) FAQs* (last modified Nov. 30, 2022), https://www.sec.gov/enforce/certaincybersecurity-related-events-faqs.

As to the fraud and false statement claims, the SEC alleges, first, that SolarWinds' risk disclosures were misleading because it supposedly had various cybersecurity deficiencies that made it not merely vulnerable, but "very vulnerable" to, or at "increased risk" of, attack. ¶¶ 243-44. Second, the SEC alleges that SolarWinds' initial 8-K about SUNBURST misleadingly omitted that SolarWinds had linked SUNBURST to certain previous customer support incidents (the same ones mentioned in the Company's follow-up 8-K four weeks later). ¶¶ 310-12. Third, the SEC alleges SolarWinds misrepresented its security policies in the Security Statement and various blogs, press releases, and podcasts. ¶ 232. As to disclosure controls, the SEC alleges the Company lacked reasonable controls for escalating potentially material incidents to senior management. ¶¶ 327-28. As to internal accounting controls, the SEC alleges that SolarWinds lacked reasonable controls to restrict access to its "information technology network environment, source code, and products," which it describes as "the Company's most critical assets." ¶¶ 320-22.

LEGAL STANDARDS

Under Rule 12(b)(6), courts accept well-pled factual allegations as true, but "the Federal Rules do not require courts to credit a complaint's conclusory statements without reference to its factual context." *Ashcroft v. Iqbal*, 556 U.S. 662, 686 (2009). "[W]here a conclusory allegation in the complaint is contradicted" by a properly considered document, "the document controls and the allegation is not accepted as true." *Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 147 (2d Cir. 2011); *see Gillis v. QRX Pharma*, 197 F.Supp.3d 557, 583–84 (S.D.N.Y. 2016) (Engelmayer, J.) (rejecting fraud claims premised on mischaracterized document).

Under Rule 9(b), a complaint must "state with particularity the circumstances constituting" alleged fraud—a standard that fully applies to SEC enforcement actions. *SEC v. Rio Tinto plc*, 2019 WL 1244933, at *6 (S.D.N.Y. Mar. 18, 2019). Thus, the SEC must "(1) specify the statements that [it] contends were fraudulent, (2) identify the speaker, (3) state where and when

the statements were made, and (4) explain why the statements were fraudulent," and also "allege facts giving rise to a 'strong inference of fraudulent intent.'" *Novak v. Kasaks*, 216 F.3d 300, 306 (2d Cir. 2000). This standard also applies to non-fraud claims "premised on allegations of fraud," *Rombach v. Chang*, 355 F.3d 164, 171 (2d Cir. 2004), where they allege the same "false and misleading statements and omissions" and "pertain to the exact same underlying events," *Lighthouse Fin. Grp. v. Royal Bank of Scot. Grp., PLC*, 902 F.Supp.2d 329, 339 (S.D.N.Y. 2012).

ARGUMENT

I. The Fraud and False-Filing Claims Should Be Dismissed

A claim for securities fraud under Exchange Act § 10(b) and Rule 10b–5 requires that Defendants "(1) made a material misrepresentation or a material omission as to which [they] had a duty to speak[]; (2) with scienter; (3) in connection with the purchase or sale of securities." *SEC v. Monarch Funding Corp.*, 192 F.3d 295, 308 (2d Cir. 1999). Securities Act § 17(a) requires largely the same elements, except negligence suffices. *Id.* A false-filing claim under Exchange Act § 13(a) requires material misstatements specifically in SEC filings, but not scienter. *Rio Tinto plc*, 2019 WL 1244933, at *17. Here, all these claims fail because the SEC does not plausibly allege any material misstatements, or any deceptive scheme based on those alleged misstatements. And the fraud claims doubly fail because they do not adequately allege scienter (or even negligence).

A. The SEC Fails to Allege a Material Misrepresentation or Omission

The SEC bases its fraud and false-statement claims on three categories of statements: (1) statements to investors in its risk disclosures before SUNBURST; (2) statements to investors after SUNBURST about the attack; and (3) cybersecurity-related statements on the Company's website and elsewhere. It fails to plausibly allege that any were materially misleading.

1. The Risk Disclosures Were Not Materially Misleading

Perhaps the SEC's most puzzling claim is that SolarWinds' risk disclosures before

SUNBURST were somehow materially misleading. The disclosures in fact warned investors of the precise risk that ultimately materialized: They specifically warned that SolarWinds' systems were "vulnerable" to various cyber threats, including "advanced persistent threat intrusions" from "sophisticated nation-state and nation-state-supported actors." ¶ 240; Ex. 1 at 2. The Company further warned that it may be unable to stop an attack "[d]espite our security measures," and that these "security problems" could lead to various material consequences, including "damage to our own systems or our customers' IT infrastructure or the loss or theft of our customers' proprietary or other sensitive information." *Id.* Any reasonable investor reading these disclosures would have understood that SolarWinds was vulnerable to a cyberattack—including one like SUNBURST. Where a company's disclosures "were sufficient to pick up the ... risk that later materialized"—as these disclosures were—as a matter of law they cannot be materially misleading. *Garnett v. RLX Tech. Inc.*, 632 F.Supp.3d 574, 602 (S.D.N.Y. 2022) (Engelmayer, J.).

Courts have found similar cybersecurity risk disclosures unactionable for this very reason. For example, in *In re Qudian Inc. Securities Litigation*, Judge Furman rejected a claim that the defendant had misrepresented its cybersecurity protocols, finding that, whatever affirmative representations the defendant made about its security measures, its offering materials plainly disclosed that those "security measures could be breached," that the defendant "may be unable ... to implement adequate preventative measures" to stop an attack, and that material consequences could ensue. 2019 WL 4735376, at *8 (S.D.N.Y. Sept. 27, 2019). "In light of these disclosures," the court held, "it cannot be said that Plaintiffs plausibly identify a material misrepresentation." *Id.*; *see also In re Equifax Inc. Sec. Litig.*, 357 F.Supp.3d 1189, 1226–27 (N.D. Ga. 2019) (finding statement that systems "could be vulnerable to ... breaches of confidential information" was not actionable, as it "warned of the precise risk that caused the Plaintiff's losses"). So too here.

The SEC articulates no coherent theory as to how SolarWinds' risk disclosures were misleading or exactly what else SolarWinds should have said. Instead, the SEC vaguely complains that the disclosures were "generic," ¶ 9, "boilerplate," ¶ 239, or "hypothetical," ¶ 9. But "[t]hese statements conveyed substantive information about the risk that ultimately materialized. As such, they were meaningful cautionary language, not mere boilerplate." *In re Sanofi Sec. Litig.*, 87 F.Supp.3d 510, 536 (S.D.N.Y. 2015) (Engelmayer, J.); *see also Rombach*, 355 F.3d at 175 (affirming dismissal where "some of the[] cautionary statements were formulaic" but "as a whole they provided a sobering picture"). Nor were the disclosures "hypothetical": they made clear the Company was *actually, presently* at risk of a cyberattack, explicitly stating that its systems "*are* vulnerable." Thus, a reasonable investor could not have been "misled into thinking that the risk that materialized"—the risk of an attack like SUNBURST—"did not actually exist." *In re FBR Inc. Sec. Litig.*, 544 F.Supp.2d 346, 361 (S.D.N.Y. 2008).

Still, the SEC insists that something was missing from the risk disclosures—it just cannot put its finger on what it was. It cycles through various allegations of "red flags," ¶ 252, claiming that SolarWinds failed to "disclose[] that known, unremediated issues with NIST Cybersecurity Framework compliance, [secure development lifecycle], network monitoring, access controls (including [a] VPN security gap), or passwords existed," ¶ 244, or that there was a "backlog" of product vulnerabilities at one point and "inadequate staffing" to address them, ¶ 296, or that SolarWinds was "[unable] to determine the root cause" of a customer-reported incident in June 2020, ¶ 270, or that a similar issue was reported in October 2020 that it likewise could not resolve, ¶¶ 280, 284. In short, the SEC seems to believe that SolarWinds had a duty to disclose detailed information about supposed cybersecurity shortcomings, and that omitting such details from its risk disclosures was materially misleading.

SolarWinds emphatically disagrees with the SEC's allegations about these supposed "issues," but even accepting the allegations as true for purposes of this motion, the SEC's disclosure theory fails as a matter of law. SolarWinds had no duty to supplement its risk disclosure with granular cybersecurity concerns or day-to-day matters such as staffing levels. "A company is generally not obligated to disclose internal problems because the securities laws do not require management to bury the shareholders in internal details, and because public disclosure of internal management and engineering problems falls outside the securities laws." *In re N. Telecom Ltd. Sec. Litig.*, 116 F.Supp.2d 446, 459 (S.D.N.Y. 2000) (quotation marks omitted). Rather, the SEC's rules require disclosure only of "the most significant factors that make an offering speculative or risky." Regulation S-K Item 503(c), 84 Fed. Reg. 12674, 12702 (Apr. 2, 2019).

SolarWinds did disclose its "most significant" cybersecurity risks: the risk of a successful attack and the material consequences that could ensue. ¶ 240. By comparison, alleged "internal problems," such as an engineer's concern about a VPN configuration or a security team's inability to resolve a customer report, cannot plausibly constitute "the most significant factors" making investment in the Company risky. Security concerns and challenges arise *routinely* in the daily operation of a cybersecurity program; enumerating them in investor filings would create a level of noise that would render the filings useless. *See In re Intel Corp. Sec. Litig.*, 2019 WL 1427660, at *13 n.17 (N.D. Cal. Mar. 29, 2019) (no duty to disclose specific vulnerabilities in computer chips); *In re N. Telecom Ltd.*, 116 F.Supp.2d at 459 (no duty to disclose "software and customer problems"); *see also Tongue v. Sanofi*, 816 F.3d 199, 214 (2d Cir. 2016) ("[S]ecurities law does not impose on [issuers] an obligation to disclose every piece of information in their possession.").[4]

[4] The allegations in the AC that certain stock analysts "would have liked to know" such information, ¶¶ 55, 69, 137, 144-45, 157, 214, do not advance the SEC's position. "[A] corporation is not required to disclose a fact merely because a reasonable investor would very much like to know that fact. Rather, an omission is

Not only did SolarWinds have no standalone duty to disclose such information, but omitting it did not render the risk disclosures misleading. Having categorically disclosed it was vulnerable to cyberattack, SolarWinds did not have to detail *how* it might be vulnerable. That information would have been merely cumulative of—not contrary to—the risk SolarWinds already disclosed. Indeed, the SEC acknowledges that the alleged vulnerabilities it cites "may not each have risen to the level of requiring disclosure on their own," asserting instead that they somehow needed to be disclosed "collectively." ¶ 243. But the "collective" risk of any vulnerabilities—the risk of a cyberattack—is exactly what SolarWinds *did* disclose. No reasonable investor would view the omitted details "as having significantly altered the 'total mix' of information made available." *Basic Inc. v. Levinson*, 485 U.S. 224, 231–32 (1988); *see In re Intel*, 2019 WL 1427660, at *11, *13 n.17 (finding "reasonable investors would not be misled" by omission of information about specific vulnerabilities "given the total mix of information" available, including broad warnings in risk disclosures); *Ong v. Chipotle Mexican Grill, Inc.*, 294 F.Supp.3d 199, 23 (S.D.N.Y. 2018) ("Having addressed these issues in general terms, Defendants did not omit material facts by failing to address, in more granular terms, every eventuality."); *In re Bank of Am. AIG Disclosure Sec. Litig.*, 980 F.Supp.2d 564, 579 (S.D.N.Y. 2013) ("[W]here there is disclosure that is broad enough to cover a specific risk, the disclosure is not misleading simply because it fails to discuss the specific risk."), *aff'd*, 566 F.App'x 93 (2d Cir. 2014); *City of Austin Police Ret. Sys. v. Kinross Gold Corp.*, 957 F.Supp.2d 277, 303 (S.D.N.Y. 2013) (Engelmayer, J.) (warnings about viability of mining operations were "sufficiently comprehensive" to cover specific risk that materialized).

Besides being unsupported by the law, the SEC's position that companies must disclose detailed vulnerability information is impractical and dangerous. No company ever achieves a state

actionable under the securities laws only when the corporation is subject to a duty to disclose the omitted facts." *In re Time Warner Inc. Sec. Litig.*, 9 F.3d 259, 267 (2d Cir. 1993).

of perfect security. *Every* company *always* has various cybersecurity risks to address and problems to fix, which evolve on a daily basis. Requiring companies to keep the investing public constantly apprised of these granular risks would be an impossible task that would "bury the shareholders in an avalanche of trivial information." *Basic Inc.*, 485 U.S. at 231–32. Not only that, but such a duty would put companies' security at risk by exposing internal cybersecurity information to hackers, who could leverage it for malicious purposes—to the ultimate detriment of investors.

The SEC itself has recognized the folly of requiring companies to disclose detailed vulnerability information, including in guidance on cybersecurity disclosures operative during the Relevant Period, which stated:

> This guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts—for example, by providing a "roadmap" for those who seek to penetrate a company's security protections. We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident.

SEC, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Rel. Nos. 33-10459 & 34-82746, at 11 (Feb. 26, 2018), https://www.sec.gov/files/rules/interp/2018/33-10459.pdf. Yet by faulting SolarWinds for failing to disclose such alleged issues as a weakness in its VPN configuration, or a failure to enforce strong passwords, the SEC is effectively asserting a new standard requiring disclosure of precisely the sort of "roadmap" information that its own guidance acknowledged would be inimical to security.[5]

[5] Even in new cybersecurity-related disclosure rules that the SEC promulgated only last year, the SEC specifically declined to require companies to disclose specifics about their cybersecurity "policies and procedures," as it sought to "avoid levels of detail that may go beyond information that is material to investors" and to "address commenters' concerns that those details could increase a company's vulnerability to cyberattack." SEC, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Rel. Nos. 33-11216 & 34-97989, at 61 (Sept. 5, 2023), https://www.sec.gov/files/rules/final/2023/33-11216.pdf. The SEC is effectively seeking here to impose more demanding disclosure rules than the ones it was able to establish through rulemaking—*after* the Relevant Period.

Perhaps anticipating this criticism, the SEC outlines a fallback position: Instead of asserting that SolarWinds' disclosures should have included more details, it asserts they should have included more descriptors. The SEC faults the Company for failing to disclose that it was not merely "vulnerable" but "very vulnerable" to attack, or that it faced an "increasing" risk of attack. ¶¶ 1, 244. But securities law "is not concerned with such subtle disagreements over adjectives and semantics." *Kinross Gold Corp.*, 957 F.Supp.2d at 298. As long as the fundamental risk has been disclosed—as it was here—the wordsmithing is immaterial. *See In re ProShares Tr. Sec. Litig.*, 728 F.3d 96, 103 (2d Cir. 2013) (rejecting attempt to "use a linguistic preference to read out of the [disclosures] a scenario which the ... disclosures clearly contemplate"); *Hill v. Gozani*, 638 F.3d 40, 60 (1st Cir. 2011) ("To the extent that the plaintiff's complaint is that the precise degree of risk was not stated, that failure is not sufficient to have rendered the statements misleading."); *In re Equifax*, 357 F.Supp.3d at 1227 ("The difference between disclosing that Equifax 'could be vulnerable' and that it was 'highly vulnerable' would not mislead a reasonable investor.").[6]

Moreover, even this fallback position is impractical and dangerous. There is no defined standard by which companies can rate themselves as "vulnerable" versus "very vulnerable" (or "very, *very* vulnerable"), or their cybersecurity risks as "steady" versus "increasing" (or "sharply increasing," and so on). Requiring companies to attempt such distinctions would require them to feign an exactitude that does not exist. *That* would be misleading to investors. *See Kinross Gold Corp.*, 957 F.Supp.2d at 298 (dismissing claim that defendant should have said "very hard" instead of "relatively hard," as these were not "industry terms of art that have fixed meanings"). Such

[6] The SEC's allegation that SolarWinds should have disclosed it faced an "increasing" risk of attack also ignores that the Company specifically disclosed that "[t]he risk of a security breach … *has generally increased*" as "the number, intensity and sophistication of attempted attacks, and intrusions from around the world *have increased*." ¶ 240 (emphasis added). Whatever difference the SEC might perceive between this disclosure and its preferred wording is too trivial to be material.

information could also be leveraged for harmful purposes, as companies that rated themselves with the most alarming descriptors would stand out as the most promising targets for cyberattacks.

Unable to articulate a plausible criticism of the risk disclosure itself, the SEC adds a *further* fallback position in the AC: It now alleges the risk disclosure was misleading because the Company allegedly made *other* "statements casting its cybersecurity practices in a positive light," *i.e.,* statements made in the Security Statement. ¶ 245. The new theory seems to be that it was misleading to make *those* statements unless SolarWinds corrected them in its risk disclosure by detailing the supposed "cybersecurity failures" that allegedly made them false. ¶ 245. But this theory merely repackages the SEC's allegations about the Security Statement. Those allegations, which are baseless as explained below, *see* pt. I.A.3, do not somehow transform the risk disclosure into an actionable statement. Even if any statements in the Security Statement were materially misleading—which they were not—that would merely imply that *those* statements needed to be corrected, not that the risk disclosure needed to be. The risk disclosure itself said nothing "positive" about SolarWinds' cybersecurity measures; to the contrary, it emphasized that the Company was vulnerable "despite our security measures." Ex. 1 at 3. The SEC's new theory thus still fails to explain how the risk disclosure itself could be misleading. *See Kocourek v. Shrader*, 391 F.Supp.3d 308, 330 (S.D.N.Y. 2019) ("statements of fact on a certain topic" are not "automatically render[ed] … misleading due to the omission of another fact concerning the same topic").[7]

2. The SUNBURST Disclosure Was Not Materially Misleading

The SEC also challenges SolarWinds' initial Form 8-K about SUNBURST, but its criticism amounts to more nitpicking that fails to plausibly allege any materially misleading statement.

[7] The SEC tries to pad its allegations with legal phraseology, accusing SolarWinds of "putting forth a total mix of information ... that painted a materially misleading picture of the risks." ¶ 249. The phrase "total mix of information" is a materiality standard, not something SolarWinds "put[s] forth," and the SEC's vague allegation of a "total mix of information" painting a "misleading picture" is no replacement for a particularized explanation of how the risk disclosure was supposedly inaccurate, as Rule 9(b) requires.

First, the SEC critiques SolarWinds' statement that SUNBURST, "if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run," asserting SolarWinds should have said that SUNBURST "definitively allowed" an attacker to compromise a customer's Orion server. ¶ 310. But the statement in the 8-K was indisputably true—SUNBURST *could* allow an attacker to compromise a customer's Orion server—and the SEC alleges no facts that would render it misleading. As the SEC acknowledges, SUNBURST merely provided a "*backdoor* into the network environments of SolarWinds' customers who downloaded and installed the infected versions of the software to systems that were *connected to the internet*." ¶ 258 (emphasis added). The presence of this downloaded backdoor on a customer's Orion server did not mean it would—or even could—actually be utilized by the attacker. For one thing, if the server were not at least "connected to the internet," the attacker would not be able to access the server at all, including the backdoor on it.[8] The SEC concedes as much, stating that SUNBURST allowed for compromise "when downloaded, installed, and connected to the internet," ¶ 310—leaving little meaningful gap between the SEC's desired language and what SolarWinds said. But this acknowledgment still does not go far enough, because even if a customer's Orion server *were* internet-connected, the customer could have controls in place blocking the attacker from accessing it—such as a firewall only allowing connections from whitelisted IP addresses. Given these possible scenarios, the statement that SUNBURST "could potentially" allow an Orion server to be compromised was not misleading, and the SEC's preference for starker (and in fact inaccurate) language cannot serve as a basis for liability. *See Singh v. Schikan*, 106 F.Supp.3d 439, 448 (S.D.N.Y. 2015) ("[C]ompanies need not depict facts in a negative or pejorative light or draw

[8] Nor does the Complaint allege Orion must run on an internet-connected server. *See id.; see also* SolarWinds, *FAQ: Security Advisory*, at Question 2, https://www.solarwinds.com/sa-overview/securityadvisory/faq#question2 (last updated Apr. 6, 2021) ("The Orion Platform is fully functional without an internet connection.").

negative inferences to have made adequate disclosures.").

Second, the SEC faults SolarWinds for two statements in the 8-K asserting that the Company was "still investigating" whether SUNBURST was successfully "exploited" as "a point of any infiltration of any customer systems." ¶¶ 311-12. The SEC contends these statements were false because, as of the filing of the 8-K, Mr. Brown allegedly had mentally "linked" two earlier-reported customer incidents to SUNBURST. ¶ 307. There is no contradiction, however, between this allegation and the challenged statement.

To begin with, the SEC fails to allege facts sufficient to show that, in "linking" the two earlier customer reports to SUNBURST, Mr. Brown believed SUNBURST was successfully "exploited" as a point of "infiltration" of either customer. The SEC glosses over a key distinction: Again, SUNBURST could be present on a customer's Orion server without being successfully exploited to infiltrate the customer's network—*i.e.*, without the attacker *entering* that "backdoor" and accessing the rest of the "house." As the SEC notes, the threat actor "utilized" SUNBURST to conduct attacks only "on approximately 100 of the 18,000" customers who downloaded the infected software. ¶ 258. The SEC makes no specific allegations the threat actor *exploited* SUNBURST in this way to *infiltrate* the networks of either of the two customers who previously reported suspicious activity to SolarWinds—much less that Mr. Brown *knew* this by the time of the 8-K.[9] Indeed, the customer involved in one of the two earlier-reported incidents, Palo Alto Networks, itself publicly stated after SUNBURST was discovered that its security controls had

[9] The SEC alleges no facts implying that the suspicious activity reported in the incidents indicated such exploitation, as opposed to the mere presence of the backdoor on the customers' Orion servers. While the SEC alleges that the customer reports involved information being sent between the customer's infected Orion server and the attacker's external infrastructure, ¶ 313, the SEC does not allege that the threat actor ever successfully used the server to pivot to other parts of the customer's network. As the federal government has noted, the backdoor would independently generate activity on a victim's infected Orion server, regardless of any exploitation, including beaconing out to the threat actor's infrastructure to signal that it was present on the system. *See* GAO Report at 14–16 & fig. 2.

"successfully prevent[ed]" the "compromise" of its network by the threat actor, underscoring the distinction between having the backdoor on the Orion server and having one's IT system "infiltrated" through "exploiting" the backdoor.[10] In light of that distinction, the SEC cannot claim that SolarWinds' use of these terms was misleading. *See Wochos v. Tesla, Inc.*, 985 F.3d 1180, 1194 (9th Cir. 2021) (no misrepresentation where complaint failed "to plead sufficient facts to establish that the actual term used had the distinctive, and false, meaning that Plaintiffs claim").

In any event, whatever Mr. Brown's understanding was at the time of the 8-K as to whether any customers had been exploited and infiltrated via SUNBURST, the SEC concedes that *the Company* "still had more investigating to do." ¶ 313. After all, the 8-K was filed the first business day after the Company learned about SUNBURST. ¶¶ 308-09. Whatever suspicions any individual employees might have had at that point, SolarWinds was entitled, and would be expected, to conduct a more thorough and formal investigation before reaching any definitive conclusions. As the 8-K asserted (and the SEC does not question), upon learning of SUNBURST, the Company immediately "retained third-party cybersecurity experts to assist in an investigation of these matters." ¶ 311; Ex. 2 at 3. That investigation barely had time to get off the ground when the 8-K was issued. The Complaint thus cannot plausibly allege that SolarWinds and its third-party experts were *not* "still investigating" whether and to what extent any customers were successfully infiltrated; and Mr. Brown's alleged beliefs about a "link[]," ¶ 307, hardly preclude that possibility. *See Gillis*, 197 F.Supp.3d at 597 (dismissing claim where "the information which the [complaint] faults defendants for omitting does not contradict the[ir] statements").

More fundamentally, the SEC does not plausibly explain why either supposed misstatement in the 8-K—that SUNBURST "could allow" an attacker to compromise a customer's

[10] Palo Alto Networks, *Rapid Response: Navigating the SolarStorm Attack* (Dec. 17, 2020), https://www.paloaltonetworks.com/blog/2020/12/solarwinds-statement-solarstorm.

Orion server, or that SolarWinds was "still investigating" whether any customers had been "infiltrated"—is material. The SEC asserts that the 8-K "failed to disclose ... the true impact of SUNBURST," ¶ 314, but that is plainly wrong. The 8-K explained that: (i) a vulnerability had been inserted into Orion, likely "by an outside nation state" as part of a "highly sophisticated ... supply chain attack"; (ii) SUNBURST had been live since March 2020, meaning the attacker had had nine months to exploit it; (iii) *as many as 18,000* SolarWinds customers had downloaded the infected software in the interim; (iv) revenue from Orion represented 45 percent of total corporate revenue; and (v) there were "numerous financial, legal, reputational and other risks to SolarWinds" as a result of all this, which the disclosure enumerated. Ex. 2 at 3. And far from suggesting the threat of customer attacks was merely "theoretical," ¶ 310, the 8-K specifically noted "significant media coverage of attacks on U.S. governmental agencies and other companies, with many of those reports attributing those attacks to a vulnerability in the Orion products," Ex. 2 at 3.

Against those sobering disclosures, the alleged omission—that a mere *two* of the 18,000 potentially affected customers had previously reported incidents suspected to be "linked" to SUNBURST—was insignificant. The disclosure that up to 18,000 customers were at risk was far more revealing of the scope of the incident. Indeed, this outer-bound figure vastly *overstated* the effect of the incident, as the number of customers actually attacked turned out to be much smaller, on the order of 100. ¶ 258. In short, the alleged omissions would not have significantly altered the total mix of information, which already made clear that SUNBURST was a serious incident that exposed many customers to potential infiltration by a sophisticated nation-state actor. *See In re Citigroup, Inc. Sec. Litig.*, 330 F.Supp.2d 367, 378 (S.D.N.Y. 2004) (dismissing claim where omission was not "material in the context of [defendant]'s overall business"), *aff'd*, 165 F.App'x 928 (2d Cir. 2006); *cf. Beleson v. Schwartz*, 419 F.App'x 38, 40 (2d Cir. 2011) (fact of impending

bankruptcy immaterial given disclosure that company had lost over $500 million, which "adequately informed [investors] of the dire nature of [its] financial condition").

The fact that SolarWinds' stock price lost nearly a quarter of its value in the wake of the initial 8-K, ¶ 318, only confirms that it made the gravity of the situation clear. By comparison, when the Company disclosed the two prior customer reports in its January 8-K a few weeks later, the stock price barely moved, and even rose in the following days. *See* Ex. 6. "That the market did not react to [the allegedly omitted information] underscores that no reasonable investor would have considered such information material." *In re Bank of Am*, 980 F.Supp.2d at 578.

3. The Security Policy Statements Were Not Materially Misleading

Lacking any basis to allege that SolarWinds' statements directed to investors were materially misleading, the SEC searches out fodder for its lawsuit elsewhere, citing various statements about SolarWinds' security policies directed to *customers*—mainly in the Security Statement posted on the Company's website. Ex. 5. Evidently trying to compensate for shortcomings identified in Defendants' initial motion to dismiss, the SEC has gone to great lengths in the AC—*literally*, adding nearly fifty pages to the document—in an effort to prop up its allegations about the Security Statement. But it is the quality, not quantity, of the allegations that matters, and that still falls short. The SEC stakes its case on the premise that there were not simply "isolated failures" in SolarWinds' implementation of the policies articulated in the Security Statement—a tacit acknowledgment that such failures would not be enough to make the policies "false." Instead, the SEC alleges there were "pervasive," "systemic," "programmatic," "years-long" failures, stretching "across wide swaths of SolarWinds or even the entire Company" and lasting "throughout the Relevant Period." ¶¶ 2, 8, 73. The actual *facts* it alleges, however, fail to support this otherwise conclusory—and extreme—assertion.

Having no witness who ever made such a claim during its lengthy investigation, the SEC relies exclusively on snippets pulled out of context from a handful of the approximately 150,000 documents it collected from the Company, which it tries to pass off as reflecting "pervasive" failures during the Relevant Period. They do not. Many of the documents cited are from before the Relevant Period, when by definition the Security Statement could not have misled investors, because SolarWinds *had* no public investors at the time.[11] As to documents from within the Relevant Period, the SEC repeatedly makes allegations that are contradicted by the very documents it cites or others on which the AC relies. *See Amidax Trading Grp.*, 671 F.3d at 147 ("[W]here a conclusory allegation in the complaint is contradicted by a document attached to the complaint, the document controls and the allegation is not accepted as true."). When stripped of these misleading allegations, the AC does not plausibly allege any "pervasive" failure to implement any policies in the Security Statement. At most, the alleged facts indicate that SolarWinds identified gaps in its policies from time to time for purposes of continually improving its cybersecurity posture—which is fully consistent with the Security Statement and with what reasonable investors would expect. *See In re Braskem S.A. Sec. Litig.*, 246 F.Supp.3d 731, 756 (S.D.N.Y. 2017) (Engelmayer, J.) ("There is an important difference between a company's announcing rules forbidding bribery and its factually representing that no officer has engaged in such forbidden conduct."); *In re Constellation Energy Grp., Inc. Sec. Litig.*, 738 F.Supp.2d 614, 631 (D. Md. 2010) ("A reasonable investor could not assume" from statements about internal controls "that the company would never lapse in these tasks.").

The SEC focuses specifically on statements within the Security Statement about: (1) the NIST Cybersecurity Framework ("NIST CSF"); (2) a secure development lifecycle ("SDL"); (3)

[11] The SEC appears to concede that conduct that predates SolarWinds' IPO cannot demonstrate falsity. *See* ¶ 67 (arguing only that material predating the Company's IPO is relevant to state of mind).

network monitoring; (4) password policies; and (5) access controls. Beyond that, the SEC cites: (6) statements made in certain blogs, podcasts, and press releases; and (7) purported evidence of a "systemic cybersecurity problem." As explained below, none of the cited statements are plausibly alleged to be misleading—let alone material.

NIST CSF Statement. The SEC first alleges that SolarWinds' statement that it "follows the NIST Cybersecurity Framework" was "false," on the basis that the Company supposedly gave itself "pervasive[ly] low scores" on its NIST CSF assessments. ¶¶ 76, 91. This allegation is fundamentally flawed: Following the NIST CSF does not require meeting any particular scores, nor does the SEC allege otherwise. As the NIST CSF itself states, it is a "voluntary" and "flexible" framework that companies use "to help them identify, assess, and manage cyber risks"—not "a one-size-fits-all approach" with specific mandates or minimum requirements.[12]

The AC explains what following the NIST CSF means: "Companies using the NIST Cybersecurity Framework generally measure themselves on a scale of 0 to 5 in five main areas relating to cybersecurity: Identify, Detect, Protect, Respond, and Recover. … These ratings are sometimes referred to as 'NIST Scorecards.'" ¶ 75. The AC makes clear SolarWinds did just that—use the NIST CSF to measure itself—throughout the Relevant Period. *See, e.g.*, ¶ 77 (SolarWinds "evaluat[ed] its internal cybersecurity practices" using NIST CSF); ¶¶ 89-91 (discussing "NIST [CSF] assessments" presented to senior executives); ¶ 95 (noting that "NIST [CSF] scorecards [were] featured prominently in many internal presentations"). The SEC therefore has no basis to allege that the statement about NIST CSF in the Security Statement was false or misleading. Because SolarWinds "made no characterization at all with respect to the quality of its

[12] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, at v–vi; *see also* ¶ 74 (describing NIST CSF as "a set of tools that an organization can use as one part of its assessment of its cybersecurity posture").

cybersecurity" in stating that it followed the NIST CSF, how high or low it scored itself has no bearing on the truth of the statement. *In re Marriott Int'l, Inc*., 31 F.4th 898, 903 (4th Cir. 2022).

But to set the record straight, the SEC's allegations that SolarWinds gave itself "pervasive low scores" in its NIST CSF self-assessments are manifestly wrong, as they are contradicted by the very "NIST Scorecards" the SEC alleges the Company used to score itself during the Relevant Period. ¶¶ 75, 89. Those scorecards show that SolarWinds' scores were not "pervasively low" but rather averaged 2.5 in 2018 and 3.0 in 2019, and were on target for 3.3 in 2020—reflecting a well-developed and consistently improving program.[13] Ex. 7 at 3 (cited in ¶¶ 90, 128); Ex. 8 at 2 (cited in ¶¶ 10(f), 198, 295); *see also* Ex. 9 (cited in ¶¶ 10, 296). The SEC ignores these inconvenient facts and instead selectively cites two "2s" and one "1" in particular segments of one scorecard, while disregarding that all the other scores on the scorecard were higher (and ignoring the scores from other scorecards it cites altogether). *Compare* ¶ 90 *with* Ex. 7. The SEC "cannot cherry-pick facts from [documents] upon which [it relies] and ignore others that contradict [its] allegations." *Chapman v. Mueller Water Prods., Inc.*, 466 F.Supp.3d 382, 391 n.3 (S.D.N.Y. 2020).

Tellingly, the SEC spends much of its NIST CSF discussion not even talking about SolarWinds' NIST Scorecards from the Relevant Period, but instead tries to change the subject to a "FedRAMP" assessment from 2019. ¶¶ 97-99. As the SEC acknowledges, that assessment was done not as part of any NIST CSF evaluation of the Company's cybersecurity posture generally, but rather "to evaluate whether certain of [SolarWinds'] *products* could be certified" under FedRAMP—a special certification program for cloud products used by the federal government. ¶ 97. The SEC tries to muddy the waters by alleging that FedRAMP incorporates "NIST 800-53"

[13] As the scorecards reflect, the scores they contain are measures of maturity, reflecting the extent to which formal documentation and compliance mechanisms are in place. In particular, a "2" reflects a "[c]onsistent approach" to applying controls that is "[s]omewhat reactive and undocumented," while a "3" reflects a "[d]ocumented, detailed approach." Ex. 8 at 2.

standards, which SolarWinds also used as part of its NIST CSF assessments—but that hardly implies the two assessments are interchangeable. And despite the SEC's attempt to blur FedRAMP and NIST 800-53 together by referring to them singularly as "FedRAMP/NIST 800-53," FedRAMP guidance makes clear that, while *based on* NIST 800-53, FedRAMP *exceeds* NIST 800-53 requirements.[14] The Security Statement said nothing about FedRAMP and the fact that the SEC raises it at all only underscores how far it is stretching to find a basis for its claims.

Secure Development Lifecycle Statement. The SEC next focuses on the Security Statement's assertion that SolarWinds "follow[s] a secure development lifecycle"—a process for developing software—that incorporates "standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments." ¶ 110; Ex. 5 at 3. The SEC alleges that "SolarWinds pervasively failed to follow an SDL during the Relevant Period," ¶ 115, but again, the allegation is directly contradicted by the documents on which the SEC relies. The SEC cites a NIST Scorecard from August 2019 listing a score of "2" for its SDL, as if it were evidence that the Company simply lacked an SDL. ¶ 128. In fact, the document makes clear (and the AC itself acknowledges) that the score means the Company had a "consistent overall approach" to ensuring that "employees are aware of and utilize a security software development lifecycle in their day to day activities," even if documentation and other formal program elements were lacking. *Id.*; Ex. 7 at 3. Thus, the document in actuality evidences that the Company *did* follow an SDL. Further, another document the SEC cites, which it describes as an "audit" from April 2018, clearly denotes, with a large green check mark, that SolarWinds had "[i]mplemented Secure Development Lifecycle." Ex. 10 (cited in ¶¶ 165, 166).

[14] *See* FedRAMP, *FAQs*, https://www.fedramp.gov/faqs (last visited Mar. 22, 2024) ("The FedRAMP security controls are based on NIST SP 800-53 baselines and contain controls, parameters and guidance *above the NIST baseline* that address the unique elements of cloud computing." (emphasis added)).

The SEC feebly tries to question the existence of the SDL by citing a June 2020 exchange about whether the SDL covered what the SEC (incorrectly) describes as a "component" of Orion, ¶ 131, but the exchange only confirms that the Company had an SDL in place and there was merely a question about how it applied.[15] It hardly provides any basis to conclude that SolarWinds "pervasively failed to follow an SDL." *See Ong*, 294 F.Supp.3d at 232 ("These allegations do not conflict with Defendants' statements regarding the … programs and procedures that Chipotle had in place, but merely quibble with Chipotle's execution of those programs and procedures.").

The SEC fares no better in alleging that SolarWinds failed to follow certain *aspects* of an SDL—in particular penetration testing, ¶¶ 110-114, which, again, the SEC's cited documents plainly indicate was part of the Company's practices. An October 2018 slide deck, for example, notes that penetration tests were "complete" for MSP and Cloud products, and that a team had already been staffed to test Orion products. Ex. 12 at 3 (cited in ¶¶ 1, 227, 241, 244, 297). The August 2019 NIST Scorecard cited by the SEC shows a score of 4 on penetration testing, with the notation: "A program for penetration testing of SolarWinds products is established and actively monitored." Ex. 7 at 6 (cited in ¶ 128). An October 2020 slide deck contains an entire slide on SolarWinds' "Penetration Testing Program" with a chart of all of the software applications that had been tested earlier that year or that were planned to be tested in the fourth quarter. Ex. 8 at 3 (cited in ¶¶ 10(f), 198, 295). It is utterly implausible for the SEC to allege in the face of these documents that SolarWinds pervasively failed to implement penetration testing as part of its SDL.

[15] The cited exchange related to the Orion Improvement Program ("OIP"). The SEC alleges that "Mr. Brown confirmed in sworn testimony that the OIP was not built under an SDL process in 2020," ¶ 133, but misleadingly omits that in the same testimony, Mr. Brown explained that OIP was not a "product[] that we sell to customers," but an application used by SolarWinds "internally" to gather usage information from customers, and for that reason was not within scope of the Company's SDL. Ex. 11 at 394:8–395:12.

Nor do the SEC's selective references to other documents provide a plausible basis to allege such a failure. One mentions a "[p]lan to PEN test 3-5 products in 2019" that was "unfunded in FY18," Ex. 13 (cited in ¶ 121); another notes a "gap" in "formalized" penetration testing (with the box shaded yellow to indicate progress was being made), Ex. 14 (cited in ¶ 121); and a third flags that "web application testing" was not "always" done before product releases, ¶ 122. But the mere fact that a particular penetration-testing project was not funded, or that penetration testing could have been more formalized, or that certain testing was not "always" done, hardly implies that there was a pervasive failure to do penetration testing at all. The SEC's effort to "construct this theory" by "cherry-pick[ing]" bits of documents amounts to nothing more than "self-serving speculation" that "falls far short of a plausible pleading, let alone one that satisfies Rule 9(b)'s requirement that fraud be pled with particularity." *Lopez v. CTPartners Exec. Search Inc.*, 173 F.Supp.3d 12, 41 (S.D.N.Y. 2016) (Engelmayer, J.); *Barker v. Bancorp, Inc.*, 2022 WL 595954, at *6 (S.D.N.Y. Feb. 25, 2022) ("The Second Circuit has cautioned district judges to be mindful of litigants who cherry-pick among relevant documents.").[16]

Network Monitoring Statement. The SEC next attacks SolarWinds' statements about network monitoring, alleging a "systemic" failure to monitor its network, but again ignoring contravening information in documents incorporated into the Complaint by reference. For

[16] The SEC also tries to make an issue of a supposed failure by SolarWinds to conduct "threat modeling" or "continuous security training." ¶ 123. But these terms are not even mentioned in the SDL Statement, which listed the specific practices encompassed by the SDL without referring to either. Ex. 5. Regardless, the SEC fails to cite any documents implying any pervasive failure to do these things during the Relevant Period. The only documents it cites from the Relevant Period specifically mentioning "threat modeling" are two product-specific assessments, and the SEC's own quotations from the documents indicate that the issues they found were deviations from "established standards" that SolarWinds otherwise followed. ¶¶ 126-27. And the allegation that SolarWinds did not conduct security training in connection with the SDL is again contravened by documents the SEC relies upon, including a May 2019 Security & Compliance presentation referring to several "training efforts that are operational," including an "annual SDL refresher." Ex. 15 (cited in ¶ 178).

example, the August 2019 NIST Scorecard cited by the SEC states that "Next Generation Firewalls"—mechanisms for monitoring network traffic[17]—were "deployed and actively monitored across the company." Ex. 7 at 5 (cited in ¶¶ 10, 89-90, 128, 192). That is *exactly* what the "Network Security" section of the Security Statement said. Ex. 5 at 2 (stating that the Company uses firewalls, including "[n]ext generation firewalls," to "monitor[] for the detection and prevention of various network security threats"). Likewise, a September 2018 slide deck cited by the SEC also notes that network firewalls were deployed, along with a "strong program" in place for "monitoring" "admin account modifications," "user permission changes," and "system changes." Ex. 16 (cited in ¶ 152) (capitalization altered).

The only document from the Relevant Period the SEC cites for its claim that SolarWinds failed to conduct network monitoring is the 2019 FedRAMP assessment, ¶ 153, which, again, related to whether certain SolarWinds *products* could be certified under FedRAMP standards. Whether SolarWinds had FedRAMP-compliant controls in place to monitor usage of these particular products provides no basis to infer that it pervasively failed to monitor activity on its own company network. *See Sjunde AP-Fonden v. Gen. Elec. Co.*, 417 F.Supp.3d 379, 396 (S.D.N.Y. 2019) (dismissing claim due to "dearth of specific allegations about … how pervasive [alleged] problems were—*e.g.*, how many models there were overall, how many were defective, what roles they played … , and what issues they were subject to"); *In re Plains All Am. Pipeline, L.P. Sec. Litig.*, 307 F.Supp.3d 583, 620–21 (S.D. Tex. 2018) (failures to implement programs in some areas of business "do not undermine the general proposition that [the defendant] ... had and implemented programs").

[17] *See, e.g.*, Cisco, *What is a Firewall?*, https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (last visited Mar. 22, 2024) ("A firewall is a network security device that monitors incoming and outgoing network traffic.")

Password Statement. The SEC next challenges the Security Statement's reference to the Company's password policy, alleging it was false because "SolarWinds failed to enforce or comply with its own password policy on multiple occasions." ¶ 163 (capitalization altered). Again, the SEC fails to allege facts showing any pervasive failure to implement its password policy. The documents cited by the SEC from within the Relevant Period convey, at most, that there were certain "situations where 'password requirements were not met,'" ¶ 168, certain "systems" where passwords were not automatically required to have certain parameters, ¶ 169, and no "automated tools" for password authentication, ¶ 171. The Security Statement said nothing about "automated tools" being used for password authentication, and mere implementation gaps with respect to certain "situations" or "systems" do not make a policy statement "false." No reasonable investor would construe the policy statement as "a guarantee" that the Company would "prevent failures in its ... practices." *ECA & Loc. 134 IBEW Joint Pension Tr. Of Chi. v. JP Morgan Chase Co*., 553 F.3d 187, 206 (2d Cir. 2009). Indeed, the fact that the Company was identifying such deficiencies reflects that it *had* a policy in place and was working to correct any deviations from it.

Access Controls Statement. The last section of the Security Statement the SEC attacks pertains to access controls. ¶ 72. The SEC fails to allege facts showing any pervasive failure to implement the policies listed in this section during the Relevant Period.

The few documents the SEC cites from within the Relevant Period do not provide a plausible basis for such an allegation. The SEC cites a document from December 2018 with notations stating, "define standards and best practices for Role Based Access Controls and Least Privilege" and "address the use of local administrator access to non-privileged users." ¶ 191. But it ignores that the first notation was coded green and the second yellow, indicating the first task had already been completed and the second was in progress. Ex. 14; *see also* ¶ 62 (alleging that

color coding relates to the status of projects or practices); *cf.* ¶ 49 (alleging that red boxes were for items that needed "more work"). Again, this at most reflects a discrete gap that SolarWinds identified for remediation, not any pervasive failure to implement access controls. *See In re Union Carbide Class Action Sec. Litig.*, 648 F.Supp. 1322, 1328 (S.D.N.Y. 1986) (statements concerning safety controls not misleading where company "knew that there were safety defects, but that steps were being taken to remedy these difficulties").

Otherwise, the SEC cites a notation in a NIST Scorecard about access to critical systems being "inappropriate" and a "need to improve" internal processes, ¶ 192, but it does not explain what the specific issue was—let alone relate it to one of the specific access-control policies in the Security Statement. Similarly, the SEC again cites the 2019 FedRAMP assessment, asserting that it found various access controls were not in place, ¶ 193; but the only access controls it identifies related to the particular "information system"—*i.e.*, the SolarWinds *product*—the assessment concerned. ¶ 194 (listing access controls relating to "*the* information system" and certain practices of the Company with respect to *that system*). The SEC wanders even further astray by citing a document about "SolarWinds' MSP Support Portal," flagging a concern that SolarWinds support staff could directly access a "customer's environments." ¶ 197. This issue did not even involve access to SolarWinds' own "databases, systems, and environments," which was what the access controls section of the Security Statement addressed. Ex. 5 at 3. "Even if these facts were sufficiently specific to satisfy the particularity requirements, … they do not amount to 'pervasive' problems." *Hill*, 638 F.3d at 64–65 & n.7.

The SEC also tacks on allegations about a "security gap" in the Company's VPN configuration, based on the fact that employees could use personal devices for remote work, ¶¶ 201-13, but these allegations are irrelevant because the Security Statement nowhere made any

representations about the Company's VPN or personal device policies. *See* Ex. 5.

Blog Posts, Podcasts, and Press Releases. The SEC attempts to pad its false-statement allegations with statements from blog posts, podcasts, and press releases, all of which (besides not being misleading for the reasons above) are immaterial puffery. ¶ 219. These include, for example, statements that SolarWinds "protect[ed] [its] customers and their customers," ¶ 220, was "focused on heavy-duty hygiene," ¶ 221, "places a premium on the security of its products," ¶ 222, and has a "commitment to high security standards," ¶ 224. Such statements "were merely generalizations regarding [the defendant's] business practices" and are "precisely the type of 'puffery' that" the Second Circuit has "consistently held to be inactionable." *ECA*, 553 F.3d at 205–06 (finding statement that company "'set the standard' for 'integrity'" unactionable); *see also Plumber & Steamfitters Loc. 773 Pension Fund v. Danske Bank A/S*, 11 F.4th 90, 103 (2d Cir. 2021) (finding statement that defendant "takes the steps necessary to comply with internationally recognized standards" unactionable); *Lopez*, 173 F.Supp.3d at 30 (finding statements about "culture, reputation, and compliance" unactionable); *In re Intel*, 2019 WL 1427660, at *8 ("Qualitative buzzwords ... cannot form the basis of a false or misleading statement.").

"Systemic" Problem. Finally, the SEC attempts to bolster its *ipse dixit* allegations of a "pervasive" failure by vaguely asserting there was a "systemic cybersecurity problem" at SolarWinds. ¶ 226. This tactic fails too. The SEC must allege falsity with particularity, by alleging specific facts evidencing that specific statements in the Security Statement were false. Nothing the SEC alleges about a "systemic cybersecurity problem" meets this bar. To the contrary, the SEC merely continues its pattern of pulling words out of context.

Most egregiously, the SEC misleadingly portrays an October 2018 slide deck as containing a "warning" from Mr. Brown that the "[c]urrent state of security leaves us in a very vulnerable

state for our critical assets." ¶ 227. The SEC cites this statement no less than *eight times* in its AC, including in the very first paragraph. ¶¶ 1, 45, 48, 63, 227, 241, 244, 297. At no point does it ever acknowledge, however, that the quote is from a *budget request* from *August 2017*—shortly after Mr. Brown arrived at the Company. It appears on a slide entitled "A Proactive Security Model–Original plan and request from August 2017," under the caption "Risks of Non-Investment," alongside a detailed plan to address the listed risks. Ex. 12 at 2. The next two slides—both titled "A Proactive Security Model—Updated October 2018 with status"—show progress made on this plan in the interim. *Id.* at 3, 4. The slides use green and yellow font to identify numerous areas where work had been completed or significant improvements had been made—including with respect to the exact language quoted by the SEC. *Id.* at 4 (showing same quote in yellow font). Thus, context makes clear that the statement was not included in this deck as a "warning" about the "current state" of SolarWinds' cybersecurity; it was included to reflect the *progress* that had been made in implementing the security plan proposed *over a year earlier*. Rather than evidencing any "systemic cybersecurity problem," the slides reflect a systemic cybersecurity *program*, identifying risks and addressing them. *See Gissin v. Endres*, 739 F.Supp.2d 488, 506 (S.D.N.Y. 2010) (noting that "context is everything" in dismissing complaint based on material incorporated by reference).[18]

The other two documents the SEC cites as evidence of a "systemic cybersecurity problem" add nothing of substance. One email raises a concern about a need to address "security/compliance requirements" "upfront" rather than "right before or after[] a system is live," ¶ 228; but the SEC does not identify what "requirements" this referred to, much less relate them to the Security Statement; and the email is about addressing the requirements earlier in project timelines, not any

[18] The SEC pulls other snippets from this slide deck out of context in precisely the same way. *Compare* ¶ 227 *with* Ex. 12 at 2-5.

failure to implement them at all. The only other document, an instant-message exchange between two employees about trying to "keep the house from burning down," ¶¶ 229-30, may be colorful, but it is hardly illuminating. The SEC provides no context to explain what (if any) specific issue the employees were complaining about, or any basis to infer a failure to implement any specific policies in the Security Statement.

* * *

In short, notwithstanding their verbosity, the SEC's allegations are not enough to meet the requirements of Rule 9(b). When the allegations are closely examined, and those that are contradicted by incorporated documents set aside, the SEC offers no competent support for its conclusory allegation that SolarWinds had "long-standing, pervasive, systemic, and material cybersecurity deficiencies" that rendered its stated security policies false. ¶ 2. At most, the only inference supported by the plausibly alleged facts is that SolarWinds identified gaps in its policies from time to time and sought to remediate them. That is the hallmark of a well-functioning cybersecurity program and does not render those policies materially false or misleading.

Nor could any such gaps be material given the Company's warnings to investors in its risk disclosures. As the disclosures stated, "unauthorized access to, or security breaches of, our software or systems," and the various material consequences accompanying such an incident, could occur "[*d*]*espite* our security measures." Ex. 1 at 3 (emphasis added). Thus, whatever representations the Security Statement made to customers about SolarWinds' security measures, the risk disclosures specifically warned investors that they could not rely on those measures to protect against the risks associated with a cyberattack. For this reason, too, a reasonable investor would not expect those measures to be free of deficiencies. *See In re Marriott*, 31 F.4th at 903 (rejecting claim based on data-privacy statements on website because "Marriott's risk disclosures

to the SEC—the content actually directed to investors—specifically warned that the company's systems 'may not be [sufficient]'"); *In re Intel*, 2019 WL 1427660, at *11 (rejecting claim based on statements touting security features given, *inter alia*, "the risk warnings about security vulnerabilities in Intel's SEC filings"); *In re Heartland Payment Sys., Inc. Sec. Litig.*, 2009 WL 4798148, at *5 (D.N.J. Dec. 7, 2009) (rejecting claim based on statement emphasizing company's "high level of security," given that "the cautionary statements in the Form 10–K—warning of the possibility of a breach and the consequences of such a breach—make clear that Heartland was not claiming that its security system was invulnerable"); *see also In re Allscripts, Inc. Sec. Litig*., 2001 WL 743411, at *6 (N.D. Ill. June 29, 2001) (statements "particularly" immaterial "when they appear in a venue directed toward potential customers, rather than shareholders").

B. The SEC Fails to Allege Scheme Liability

The SEC nominally asserts scheme liability as alternative to its misrepresentation theories, ¶¶ 333(a), 340(a), but the alleged "scheme" consists merely of "posting a 'Security Statement' and making other public statements that claimed SolarWinds was following good cybersecurity practices." ¶ 5; *see also* ¶¶ 10(a), 57, 64, 67, 119, 226. That is not sufficient. Scheme liability "requires something *beyond* misstatements and omissions." *SEC v. Rio Tinto plc*, 41 F.4th 47, 49 (2d Cir. 2022). There must be a separate "inherently deceptive act," such as "sham agreements, sham transactions, sham companies, or undisclosed payments." *In re Turquoise Hill Res. Ltd. Sec. Litig.*, 625 F.Supp.3d 164, 253 (S.D.N.Y. 2022). Nothing like that is alleged here. Instead the SEC merely alleges that "Brown (or others acting at his direction) disseminated the Security Statement … to customers." ¶ 58. But "dissemination" must be "distinct from an alleged misstatement" to be the basis for scheme liability, *In re Turquoise Hill*, 625 F.Supp.3d at 253, and moreover it must be "'key'" to the scheme, *id.* at 248 (quoting *Lorenzo v. SEC*, 139 S.Ct. 1094, 1101 (2019) and *Rio Tinto*, 41 F.4th at 53). The alleged dissemination here was neither of those things.

Courts "have routinely rejected the SEC's attempt to bypass the elements necessary to impose 'misstatement' liability … by labeling the alleged misconduct a 'scheme' rather than a 'misstatement.'" *SEC v. Kelly*, 817 F.Supp.2d 340, 343 (S.D.N.Y. 2011).); *see Menaldi v. Och-Ziff Cap. Mgmt. Grp. LLC*, 277 F.Supp.3d 500, 519–20 (S.D.N.Y. 2017) (plaintiff cannot merely "repackage the misrepresentation allegations" as a "scheme"). This Court should do the same here.

C. The SEC Fails to Allege a Strong Inference of Scienter

The SEC's fraud claims independently warrant dismissal because they fail to raise a "strong inference of scienter," meaning "an intent to deceive the investing public." *Acito v. Imcera Grp., Inc.*, 47 F.3d 47, 54 (2d Cir. 1995). Pleading scienter requires alleging "facts to show either (1) that defendants had the motive and opportunity to commit fraud, or (2) strong circumstantial evidence of conscious misbehavior or recklessness." *ECA*, 553 F.3d at 198.

The SEC fails to adequately allege either. The only motive to commit fraud the SEC offers—"to obtain and retain business," ¶ 46—fails as a matter of law because it can be imputed to "virtually every company," *Acito*, 47 F.3d at 54, and identifies no "concrete and personal way" in which the alleged fraud would benefit Mr. Brown or any SolarWinds executives, *Novak*, 216 F.3d at 307.[19] Given that "motive is not apparent ... the strength of the circumstantial allegations [of conscious misbehavior or recklessness] must be correspondingly greater," *Kalnit v. Eichler*,

[19] If the SEC seeks to establish motive based on Mr. Brown's stock sales during the Relevant Period, *see* ¶ 39, those allegations are also insufficient. Alleged trading does not support an inference of scienter unless the activity is "unusual." *Ark. Pub. Emps. Ret. Sys. v. Bristol-Myers Squibb Co.*, 28 F.4th 343, 355 (2d Cir. 2022). That depends, in turn, on the resulting profits, the portion of holdings involved, any change of volume in sales, the amount of insiders selling, and the timing of the sales. *See In re Aratana Therapeutics Inc. Sec. Litig.*, 315 F.Supp.3d 737, 762 (S.D.N.Y. 2018) (Engelmayer, J.). The SEC alleges no such factors here, instead only alleging the gross proceeds Mr. Brown received—which is insufficient. *See In re Skechers USA, Inc. Sec. Litig.*, 444 F.Supp.3d 498, 525 (S.D.N.Y. 2020) (holding that it is not enough to "only recite the amount of proceeds [defendant] obtained, which by itself says 'nothing about his motive'"). The fact that Mr. Brown was not even the maker of the statements in the Company's SEC filings only underscores the irrelevance of the stock sale allegations. *In re eSpeed, Inc. Sec. Litig.*, 457 F.Supp.2d 266, 289 (S.D.N.Y. 2006) (lack of stock sales by *makers* of statements undermines inference of scienter).

264 F.3d 131, 142 (2d Cir. 2001), establishing at a minimum "conscious recklessness—*i.e.*, a state of mind *approximating actual intent*, and *not merely a heightened form of negligence*," *S. Cherry St., LLC v. Hennessee Grp. LLC*, 573 F.3d 98, 109 (2d Cir. 2009). The SEC alleges no evidence of any such state of mind here. There are no emails reflecting any intentional effort to deceive or state of mind approximating that, no cooperating witnesses who have testified to any such misconduct—no evidence at all that anyone sought to do anything other than their jobs.[20] Despite years of investigation, the SEC identifies just one tangential statement that could suggest some sort of dishonesty: In a call with a customer, an unnamed "Employee F" allegedly messaged a colleague that he "just lied." ¶ 283. Putting aside that this allegation says nothing about Mr. Brown or *any* of the challenged statements, Employee F's alleged misrepresentation *to a customer* "cannot be conflated with an intent to defraud the shareholders." *Kalnit*, 264 F.3d at 141.

Nor does the picture look better for the SEC when one zooms in closer. As to each set of alleged misstatements, there are no alleged facts that could support a strong inference scienter.

1. The Risk Factor Allegations Do Not Support Scienter

Putting aside that the risk disclosures were entirely accurate, the SEC fails to adequately allege scienter on behalf of anyone involved in making them. The disclosures were made by "the Company's CEO and CFO," ¶ 239; no one else (including Mr. Brown) is alleged to have had any role in formulating or approving them. Yet the SEC pleads almost nothing about SolarWinds' CEO or CFO—certainly nothing suggesting scienter.

[20] The SEC fails to adequately plead negligence for similar reasons it fails to plead scienter: As explained below, the makers of the statements had no reason to believe the statements were incorrect, and the SEC cannot plausibly allege the Company or Mr. Brown deviated from the standard of care in light of SolarWinds' robust disclosures and efforts to enforce security policies. *See Zappia v. Myovant Scis. Ltd.*, 2023 WL 8945267, at *6 (S.D.N.Y. Dec. 28, 2023) (dismissing securities claim for failing to plausibly allege "negligent[] rather than accidental[] or reasonabl[e]" conduct).

The *only* substantive allegation about the CFO is that he "was aware" certain IT controls tested for SOX purposes were found deficient in 2019, with most remediated by March 2020 (and none alleged to have been a material weakness). ¶ 167. As for the CEO, the AC alleges merely that he was present for or "received" presentations mentioning certain alleged cybersecurity deficiencies. ¶¶ 89, 121, 168, 192, 198. These allegations do not support a strong inference that the CEO or CFO knew the risk disclosures were "false" or intended for them to deceive investors. There is an obvious benign explanation for why they would approve the risk disclosures, even if they had learned of certain deficiencies: They had no reason to believe (and are not alleged to have believed) that the deficiencies were material or that the disclosures were insufficient, especially given the disclosures' broad warning that the Company was vulnerable to cyberattack. *See In re Centerline Holdings Co. Sec. Litig.*, 613 F.Supp.2d 394, 404 (S.D.N.Y. 2009) (no strong inference where it was "arguable that [defendants] did not have a duty to disclose" omitted information), *aff'd*, 380 F.App'x 91 (2d Cir. 2010); *see also City of Philadelphia v. Fleming Cos, Inc.*, 264 F.3d 1245, 1264 (10th Cir. 2001) ("[T]he important issue in this case is *not* whether Defendants knew the underlying facts, but whether Defendants knew that not disclosing [those facts] posed substantial likelihood of misleading a reasonable investor.").[21]

The SEC also variously tries to allege scienter on the part of a "member of SolarWinds' sales team," ¶ 268, "SolarWinds and Brown," ¶¶ 232, 280, 285, 300, Mr. Brown alone, ¶¶ 175, 180, or "SolarWinds employees ... collectively," ¶¶ 237, 304, 317. But this mix-and-match strategy fails because it does not suggest that anyone who *made* the disclosure statements did so recklessly

[21] Nor does the SEC add anything by alleging that "SolarWinds executives could have reasonably anticipated that SolarWinds would be subject to a material cyberattack." ¶ 238. If that is not an impermissible "fraud by hindsight" theory, it is hard to imagine what would be. *Novak*, 216 F.3d at 309 ("[A]llegations that defendants should have anticipated future events and made certain disclosures earlier than they actually did do not suffice to make out a claim of securities fraud.").

or with intent to defraud investors. "[I]t is not enough to *separately* allege misstatements by some individuals and knowledge belonging to some others where there is no strong inference that, in fact, there was a connection between the two." *Silvercreek Mgmt., Inc. v. Citigroup, Inc.*, 248 F.Supp.3d 428, 440 (S.D.N.Y. 2017); *see Xu v. Gridsum Holding Inc.*, 624 F.Supp.3d 352, 364 (S.D.N.Y. 2022) ("the group-pleading doctrine is no longer viable"); *Nordstrom, Inc. v. Chubb & Son, Inc.*, 54 F.3d 1424, 1435 (9th Cir. 1995) (rejecting "'collective scienter' theory").

The AC tries to bridge this gap with a vague new allegation that Mr. Brown "provided information" that "others used to create risk disclosures," ¶ 242, yet it fails to identify what information was given to whom, or if it was even used to create the risk disclosure at issue. *See SEC v. Berry*, 580 F.Supp.2d 911, 922 (N.D. Cal. 2008) (allegation that defendant "'reviewed' and 'discussed' various filings is insufficient to plead (with particularity) [defendant]'s role in the purported fraud"). Indeed, the SEC admits that Mr. Brown never even read the disclosures. ¶ 242. Such formless allegations cannot carry the SEC's burden under Rule 9(b).

2. The SUNBURST Disclosure Allegations Do Not Support Scienter

The SEC does not allege a strong inference of scienter regarding the SUNBURST disclosure either. Even accepting the allegation that Mr. Brown immediately "linked" two previous customer reports to SUNBURST, ¶ 307, that does not raise a strong inference that Mr. Brown or SolarWinds sought to hide "the true impact of SUNBURST" from investors, ¶ 314. Rather, the only plausible inference is that SolarWinds did not disclose the allegedly omitted information "because it was investigating the extent of the problem." *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1065 (9th Cir. 2014); *see also Iqbal*, 556 U.S. at 680 (unlawful motive not plausibly alleged where it is merely "consistent" with facts "more likely explained by[] lawful ... behavior").

As noted above, whatever Mr. Brown might have personally suspected about whether and how SUNBURST was linked to any customer reports, the Company had only learned of

SUNBURST a mere two days before filing the initial 8-K; and it was reasonable for it to conduct further investigation, assisted by an outside forensics firm, before drawing any firm conclusions about such an issue. After all, it would not benefit investors to "jump the gun with half-formed stories." *Higginbotham v. Baxter Int'l, Inc.*, 495 F.3d 753, 761 (7th Cir. 2007). The 8-K itself said exactly that: "So as not to compromise the integrity of any investigations, SolarWinds is unable to share additional information at this time." Ex. 2 at 4. A company intending to deceive investors would not *tell them* it was withholding information. The plausible inference instead is that—just as the 8-K said—the Company was "still investigating" the issue (among many others), and simply needed more time to conduct that investigation. *See Slayton v. Am. Exp. Co.*, 604 F.3d 758, 777 (2d Cir. 2010) ("Ordering an investigation as soon as [defendants] learned [of the issue] … was a prudent course of action that weakens rather than strengthens an inference of scienter.").

This benign explanation is confirmed by the follow-up disclosure SolarWinds made only weeks later, which specifically disclosed the very "link" the SEC alleges SolarWinds sought to hide. That January 2021 8-K disclosed that SolarWinds had "identified two previous customer support incidents that, with the benefit of hindsight, we believe may be related to SUNBURST." Ex. 4 at 5. The SEC evidently recognizes that this disclosure runs counter to its fraud allegations, which is why it takes the position that this disclosure "ends the alleged scheme." Hr'g Tr. 4:21–5:8 (explaining that "at that point that is sort of enough that is revealed that the SEC is no longer alleging that the scheme continued after that point"). But the idea that SolarWinds engaged in a "scheme" to conceal information only to reveal it a few weeks later is, of course, absurd. The only plausible inference is that there was never any "scheme" to begin with. *See Gregory v. ProNAi Therapeutics Inc.*, 297 F.Supp.3d 372, 402 n.13 (S.D.N.Y. 2018) (Engelmayer, J.) (allegation that company failed to disclose drug trial results "earlier than it did" could not form basis for scienter).

Other considerations also undermine any inference of scienter: SolarWinds disclosed the attack the first trading day after learning about it, reported the maximum number of customers possibly affected, described the importance of Orion to the business, and enumerated the "numerous financial, legal, reputational and other risks to SolarWinds" emanating from the attack. Ex. 4 at 5–7. These are not the acts of a company behaving recklessly or seeking to cover up bad facts. If the Company had intended to downplay the significance of the incident, it makes no sense that it would intentionally disclose a worst-case, outer-bound figure of 18,000 potentially compromised customers, yet conceal facts about a mere two of those customers. The dissonance between the proactive steps the Company took and what it is accused of having done simply cannot be reconciled. *See Rombach*, 355 F.3d at 176–77 (proactive disclosure "weakened" inference of recklessness); *In re Bausch & Lomb, Inc. Sec. Litig.*, 592 F.Supp.2d 323, 343 (W.D.N.Y. 2008) (rejecting scienter where company "immediately launched a massive independent investigation" and "voluntarily reported the matter"); *In re Dynagas LNG Partners LP Sec. Litig.*, 504 F.Supp.3d 289, 324 (S.D.N.Y. 2020) (rejecting premise that defendants would "disclose financial information regarding the impact of the new charter contract, on the one hand, while knowingly or recklessly lying to the public about the financial state of the company, on the other").

3. The Security Policy Statement Allegations Do Not Support Scienter

Finally, the SEC does not allege a strong inference that SolarWinds or Mr. Brown sought to deceive investors through statements to customers about SolarWinds' security policies. Indeed, the SEC's scienter allegations amount to sheer conspiracy theory. The SEC alleges that Mr. Brown, immediately upon being hired in July 2017, "realized the Company's cybersecurity posture was poor," and, rather than simply working to improve the Company's cybersecurity as he was hired to do, hatched a "scheme" to deceive investors—nearly a *year-and-a-half before the Company's IPO*—by putting out a Security Statement directed to customers, certain portions of which were

allegedly false. ¶ 5. Mr. Brown is supposed to have concocted this "scheme" single-handedly—no co-conspirators are identified—even though he stood to gain no concrete personal benefit from it and was new to the Company. And he is supposed to have continued the "scheme" *for years,* intentionally continuing to "conceal SolarWinds' poor cybersecurity practices from customers and investors ... throughout the Relevant Period." ¶ 67. Fundamentally, it makes no sense that Mr. Brown, a cybersecurity professional who had no executive position at the time or any role in investor relations,[22] would decide to lie to investors about the Company's cybersecurity practices year after year, rather than simply doing his job. *In re GeoPharma, Inc. Sec. Litig.*, 411 F.Supp.2d 434, 446 n.83 (S.D.N.Y. 2006) ("Courts often refuse to infer scienter, even on a recklessness theory, when confronted with illogical allegations."); *In re Lululemon Sec. Litig.*, 14 F.Supp.3d 553, 584 (S.D.N.Y. 2014) ("It defies credulity to believe that if the fix were simply that which lead plaintiff asserts ... defendants would purposely have avoided implementing it.").

Moreover, the SEC's theory is debunked by its own documents, which reflect that Mr. Brown *was* doing his job year after year, by working to ensure the Company implemented appropriate controls, including those in the Security Statement. The Company's NIST Scorecards alone, notwithstanding the SEC's flagrant mischaracterization of them, show that it had a well-functioning and continuously improving cybersecurity program during the Relevant Period. *See* Exs. 7, 8. These same documents specifically indicate that SolarWinds had policies from the Security Statement in place, such as an SDL, penetration testing, and network monitoring. At the very least, the documents reflect that Mr. Brown, who is alleged to have prepared them, ¶ 128, *believed* these things—making it implausible to conclude that he understood (let alone *intended*) the Security Statement to be false. Likewise, to the extent that Mr. Brown's presentations contained

[22] Mr. Brown did not become CISO until January 2021. Before then, he was Vice President of Security Architecture, a non-executive position reporting to the Chief Information Officer. ¶¶ 1, 62.

information about gaps in the Company's security policies, the fact that he "routinely shared" these presentations with senior management, ¶ 168, makes it implausible to believe he sought to hide such information from investors. If he had, it would make little sense for him to regularly share the information with those in the Company actually responsible for investor disclosures.

Notwithstanding that Mr. Brown's "scheme" is supposed to have lasted for more than four years, the SEC does not cite a single document reflecting any conscious effort on his part to deceive anyone with the Security Statement or any awareness that any part of the document was false. To the contrary, the SEC alleges that Mr. Brown's first concern was to ensure the statements were "legally approved." ¶ 51. The only document the SEC cites flagging a concern about a statement in the Security Statement is a January 2018 email from an unnamed security engineer, flagging that there was "improvement needed to be able to meet the security expectations of a Security Development Lifecycle." ¶ 10(a). The SEC seizes on this email as if it were some kind of smoking gun, straining to characterize it as evidence of a "scheme" to "conceal the present falsity of the representations [in the Security Statement's SDL section] and work to make them true eventually." *Id.* But the email is not even alleged to have been received (let alone sent) by Mr. Brown, and it is from ten months before the Company's IPO. More importantly, the SEC ignores that the email reflects an effort to *ensure that SolarWinds' stated policy was being fully followed*—the very opposite of an intent to deceive. Indeed, as noted above, another document the SEC cites from only three months later (and still months before the IPO) reflects the SDL had been "implemented" by that point, Ex. 10—hardly consistent with any "scheme" to simply acquiesce in the alleged deficiency and fool investors about it, for years on end. *See In re Wachovia Equity Sec. Litig.*, 753 F.Supp.2d 326, 363 (S.D.N.Y. 2011) (no scienter based on internal policy violations where no evidence they were "knowingly sanctioned" or the product of "recklessness").

Nor can the SEC find support for its alleged "scheme" in any other documents it cites. As explained above, notwithstanding the SEC's misleading characterizations, at most the documents reflect security personnel periodically identifying gaps in SolarWinds' policies for purposes of remediating them. That does not imply that Mr. Brown (or anyone else) believed that a "policy was never followed" at all. *Lewy v. SkyPeople Fruit Juice, Inc.*, 2012 WL 3957916, at *20 (S.D.N.Y. Sept. 10, 2012); *see also In re Poseidon Concepts Sec. Litig.*, 2016 WL 3017395, at *15 (S.D.N.Y. May 24, 2016) (no scienter where auditing deficiencies did "not suggest the existence of an audit that was 'so deficient as to amount to no audit at all'"). Policies are not guarantees of perfect compliance. To the contrary, part of *having* a policy involves using it to identify and correct gaps in compliance. That process is a hallmark of a culture *of security*, rather than any corrupt "scheme." *See Sjunde AP-Fonden v. Goldman Sachs Grp., Inc.*, 545 F.Supp.3d 120, 135 (S.D.N.Y. 2021) (plaintiff "cannot have it both ways" by simultaneously arguing defendant lacked controls and had scienter based on efforts to enforce those controls).

II. The Disclosure Controls Claim Should Be Dismissed

The SEC attempts to work backward from its (flawed) omissions allegations to a disclosure controls claim, effectively arguing that because SolarWinds did not disclose everything the SEC would have liked, the Company's disclosure controls *must* have been inadequate. But the SEC's repackaged omissions theory fails under rubric of disclosure controls too.

To start with, Rule 13a–15 only requires companies to maintain controls "designed to ensure that information *required to be disclosed*" is timely reported. 17 C.F.R. § 240.13a–15(e). As explained above, the "issues" the SEC identifies—such as the "VPN vulnerability" and the two customer incident reports Mr. Brown allegedly linked to SUNBURST when it was discovered, ¶¶ 328-29—were not required to be reported in the first place. *See supra*, pt. I.A.; *In re Hebron Tech. Co., Ltd. Sec. Litig.*, 2021 WL 4341500, at *20 (S.D.N.Y. Sept. 22, 2021) (Engelmayer, J.)

(dismissing claim where alleged "disclosure lapses" were "derivative" of "ill-pled" omissions claims); *SEC v. Siebel Sys., Inc.*, 384 F.Supp.2d 694, 710 (S.D.N.Y. 2005) (dismissing disclosure controls claim premised on insufficiently alleged selective disclosure). In any event, the SEC ignores that the evidence of these "issues" cited in the AC largely consists of presentations made by Mr. Brown to upper management, *see, e.g.*, ¶¶ 192, 227, indicating that processes *were* in place to keep management apprised of cybersecurity issues.

Indeed, the SEC acknowledges that SolarWinds *had* controls to ensure disclosure, including an Incident Response Plan ("IRP") with scoring criteria for escalating potentially material incidents, ¶ 328, and it makes no claim that these criteria were unreasonably designed. Instead, the SEC chiefly complains that Mr. Brown "did not ensure that" the two customer reports were contemporaneously scored as high as the SEC believes in retrospect they "should have been." ¶¶ 273, 287. This argument, besides suffering from severe hindsight bias, finds no support in the alleged facts and does not validly state a disclosure controls violation in any event.

As the SEC alleges, when each of these incidents was originally being investigated, each was classified at level 0 under SolarWinds' IRP, ¶¶ 273, 287, designating an "undetermined security activit[y] or event[]," Ex. 17 (IRP) at 2. The SEC alleges, with the benefit of hindsight, that the reports should have each been classified as level 2, designating a "security compromise" that "affects multiple SWI customers." ¶ 328; Ex. 17 at 2. But the alleged facts make clear no one at SolarWinds contemporaneously knew that these incidents resulted from any security compromise of SolarWinds' software, or that they were part of an incident affecting multiple customers—because SolarWinds could not "determine the root cause" behind either incident. ¶¶ 270, 284. The SEC therefore has no basis to allege either incident was misclassified as "undetermined." At most, the SEC alleges that Mr. Brown believed at the time that the incidents

"*could be* part of a 'larger attack[]' campaign involving SolarWinds' flagship product that *could* affect more SolarWinds customers." ¶ 274 (emphasis added); *see also* ¶ 328 (alleging Mr. Brown believed this was "one possibility"). But the IRP did not require escalation merely if an incident *could* be a security compromise that affects multiple customers; the IRP required escalation only if it *was* such an incident. Ex. 17 at 2. (And for good reason: an amorphous escalation standard based on speculation about what an incident "could" be would lead to all sorts of incidents being escalated, flooding executives responsible for disclosures with useless noise.) Thus, Mr. Brown's contemplation of this possibility does not imply the incidents were misclassified either.[23]

Even if the SEC had any valid ground to assert that the IRP criteria was misapplied with respect to these incidents—which it does not—that would not suffice for a disclosure controls violation. Rule 13a–15 requires only that disclosure controls be appropriately designed, not that they be perfectly applied. *See In re Banco Bradesco S.A. Sec. Litig.*, 277 F.Supp.3d 600, 648 (S.D.N.Y. 2017) ("[A]llegations that those controls must have been deficient because they may have failed to detect some weaknesses in its financial reports or disclosures in some instances, are not sufficient."); *Arora v. HDFC Bank Ltd.*, 671 F.Supp.3d 305, 315 (E.D.N.Y. 2023) (dismissing claim based on internal controls because the allegations failed to explain "how or why they were deficient") (collecting cases). Nor can the SEC rely on nebulous claims of a lack of adequate "culture." ¶ 330. Rule 13a–15 has no "culture" requirement, and even if it did, the SEC does not allege any "cultural" problem, *e.g.*, that disclosure controls were willfully ignored or

[23] In yet more hindsight-biased second-guessing, the SEC criticizes Mr. Brown for not concluding by the time of the second incident that a larger attack was occurring, alleging that he should have known "that an attack [sic] was almost surely looking to use Orion in a larger attack." ¶ 286. But the point remains that no one had yet determined at the time what the root cause of either incident was, let alone that they had the *same* cause. ¶ 284. As indicated in the conversations the SEC quotes, SolarWinds was *investigating* whether the two incidents were related, but it had not been able to draw any definitive conclusion. *See, e.g.*, ¶ 280 ("This does not appear to be OIP (that we know of yet) related"); ¶ 281 ("*seems* similar to [U.S. Government Agency A] where BusinessLayer was also used to attack" (emphasis added)); *id.* ("I'm [curious] what happened on [U.S. Government Agency A] and this *could be* a way to find out." (emphasis added)).

circumvented. In short, absent some explanation of what was wrong with the *design* of the Company's disclosure controls, the SEC has no basis for a disclosure controls claim. *See Linenweber v. Sw. Airlines Co.*, 2023 WL 6149106, at *9 (N.D. Tex. Sept. 19, 2023) (dismissing claim where "[p]laintiffs have not adequately alleged that [d]efendants improperly failed to disclose any information, much less that [d]efendants' failures were so widespread as to create doubt that [d]efendants maintained disclosure controls"); *Higginbotham*, 495 F.3d at 760 (rejecting controls claim where plaintiff failed to cite any different controls that should have been in place).

III. The Internal Accounting Controls Claim Should Be Dismissed

The SEC's theory on internal accounting controls claim is not only meritless, it is a bald attempt to arrogate power Congress has not granted. Section 13(b)(2)(B) of the Exchange Act is a narrow provision requiring public companies to maintain "a system of internal accounting controls." Yet the SEC seeks to recast it as a boundless mandate for it to regulate public companies' *cybersecurity* controls—even controls for detecting *bugs in software products.* ¶ 321. Relying on a clause that requires companies to have "internal accounting controls" that reasonably safeguard "access to assets," 15 U.S.C. § 78m(b)(2)(B), the SEC contends that "SolarWinds' information technology network environment, source code, and products were among the Company's most crucial assets"—ergo, any failure to reasonably protect those "assets" from hackers constitutes an "internal accounting controls" violation. ¶ 322. This specious argument reads "accounting" right out of the statute and has no support in the text, legislative history, or caselaw.

Section 13(b)(2)(B), titled "Books, Records, and Internal Accounting," requires companies to maintain "internal accounting controls" and "books, records, and accounts" that fairly reflect their "transactions" and disposition of "assets." Specifically, it requires companies to:

> devise and maintain a system of internal *accounting* controls sufficient to provide reasonable assurances that:
> (i) *transactions* are executed in accordance with management's general or

> specific authorization;
> (ii) *transactions* are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for *assets*;
> (iii) access to *assets* is permitted only in accordance with management's general or specific authorization; and
> (iv) the recorded accountability for *assets* is compared with the existing *assets* at reasonable intervals and appropriate action is taken with respect to any differences.

15 U.S.C. § 78m(b)(2)(B) (emphasis added). This text makes clear that the provision governs only internal *accounting* controls—not internal controls generally. The text equally makes clear that the "assets" it concerns are those related to *accounting*, *i.e.*, the sort of assets that would appear on its balance sheet. Nothing in the text suggests that it covers *cybersecurity* controls over *information-technology* "assets" with no nexus to accounting. *See Saks v. Franklin Covey Co.*, 316 F.3d 337, 345 (2d Cir. 2003) ("The text's plain meaning can best be understood by looking to the statutory scheme as a whole and placing the particular provision within the context of that statute.").

The ordinary meaning of the text is confirmed by the legislative history. Congress introduced the "internal accounting controls" provision as part of the Foreign Corrupt Practices Act of 1977, which it enacted in response to concerns about "bribery of foreign officials by United States business interests." *United States v. Kay*, 359 F.3d 738, 746 (5th Cir. 2004). Congress's explicit purpose was "to strengthen the accuracy of the corporate books and records and the reliability of the audit process which constitute the foundations of our system of corporate disclosure," in order "to prevent the use of corporate assets for corrupt purposes" and to provide "assurance that corporate recordkeeping is honest." S. Rep. No. 95-114, at 7 (1977). Thus, the focus was on bookkeeping, not anything broader (and certainly not cybersecurity).

Indeed, the specific language of Section 13(b)(2)(B) comes from a Statement on Auditing Standards published by the American Institute of Certified Public Accountants (AICPA). *See id.*

at 8 (citing AICPA Statement on Auditing Standards No. 1, 320.28 (1973)). That Statement explained that "accounting controls" are limited to "the safeguarding of assets and the reliability of financial records." *Id.* at 320.28. It further explained that "safeguarding assets" in this context does not broadly mean protecting assets "against something undesirable," *id.* at 320.14, but rather means protecting assets against "loss"—of the sort that could cause *accounting* discrepancies, such as "overpayments to vendors or employees arising from inaccuracies in quantities of materials," or "physical loss of assets such as cash, securities, or inventory," *id.* at 320.15 & 320.19; *see also In re Ikon Office Sols., Inc. Sec. Litig.*, 277 F.3d 658, 672 n.14 (3d Cir. 2002) ("'Internal accounting controls' refers to the mechanism by which companies monitor their accounting system (their individualized method of processing transactions) for errors and irregularities in order to safeguard company assets and ensure that records are sufficiently reliable.").

Section 13(b)(2)(B) thus does not authorize the SEC to bring suit based on purported "shortcomings to SolarWinds' cybersecurity controls." ¶ 324. If Congress had meant to authorize the SEC to serve as some sort of roving cybersecurity commissioner for public companies, it surely would have said so in plainer terms, and there would have been some discussion of it in the legislative history. Any such mandate would have sweeping implications for public companies, as well as for the SEC—which lacks the expertise or resources to perform such a role. Congress does not legislate this way; it "does not hide elephants in mouseholes by altering the fundamental details of a regulatory scheme in vague terms of ancillary provisions." *Sackett v. EPA*, 598 U.S. 651, 667 (2023) (quotation marks omitted); *see West Virginia v. EPA*, 142 S.Ct. 2587, 2610 (2022) (courts are skeptical of "claim[s] to discover in a long-extant statute an unheralded power representing a transformative expansion in [an agency's] regulatory authority" (quotation marks omitted)).

No court has endorsed the SEC's revisionist reading of the statute. Courts have instead

uniformly dismissed Section 13(b)(2)(B) claims that are not directed at controls specifically related to *accounting*. *See, e.g.*, *SEC v. Felton*, 2021 WL 2376722, at *12 (N.D. Tex. June 10, 2021) (dismissing claim because "the SEC does not identify a single internal control that governed the handling of sales, inventory, exchanges, returns, recognition of revenue, etc." (quotation marks omitted)); *SEC v. Patel*, 2009 WL 3151143, at *26 (D.N.H. Sept. 30, 2009) (dismissing claim where allegations said "nothing about manual or automated reviews of records, methods to record transactions, reconciliation of accounting entries, or anything else that might remotely qualify as an internal accounting control"); *see also In re Equifax*, 357 F.Supp.3d at 1230 ("Even if Equifax's data breach protocol was vastly deficient, this does not establish that it had insufficient internal controls over financial reporting."). This Court should likewise dismiss the SEC's claim here.

IV. The Aiding-and-Abetting Claims Should Be Dismissed

Finally, the SEC's aiding-and-abetting claims against Mr. Brown all fail. Liability for aiding and abetting requires the knowing or reckless provision of substantial assistance to achieve a primary violation. *SEC v. Apuzzo*, 689 F.3d 204, 211 (2d Cir. 2012). The SEC fails to allege any aiding-and-abetting theory that is coherent, let alone legally sound.

The aiding-and-abetting allegations center on Mr. Brown signing certain "sub-certifications" for purposes of compliance with the Sarbanes–Oxley Act, attesting to the adequacy of certain subsets of SolarWinds' cybersecurity controls. ¶¶ 337, 344, 351, 358, 365. The theory is not pled with sufficient particularity and is difficult to discern, however, as the SEC does not explain how signing allegedly false sub-certifications would substantially assist any alleged primary violations. To be clear, the SEC does not (and cannot) allege the sub-certifications signed by Mr. Brown were directed at or disseminated to the public. Rather, the SEC merely alleges that these *internal* attestations were "relied on" by SolarWinds executives. ¶¶ 22, 298. The theory thus seems to be that Mr. Brown substantially assisted SolarWinds executives in committing primary

violations by making false statements to those executives. That is nonsense.

Substantial assistance means that the defendant "associated himself with the venture, participated in it as in something that he wished to bring about, and sought by his action to make it succeed." *Apuzzo*, 689 F.3d at 214, 217. As to the fraud and false statement claims, the SEC does not adequately allege how Mr. Brown could have "associated himself with" and "participated in" the venture, or "sought by his action to make it succeed," by making false certifications *to his principals*. The allegation is illogical: If the executives were deceived by the certifications, that would negate any scienter on their part, so there would be no primary violation in the first place. Nor does it make any sense that Mr. Brown would seek to deceive executives with internal sub-certifications while "routinely" updating those executives about cybersecurity concerns through quarterly presentations and other communications. ¶168. As to the disclosure controls claim, the primary violation is the alleged failure to maintain reasonably designed disclosure controls; but neither Mr. Brown's sub-certifications nor any other conduct alleged on his part concern the design of SolarWinds' disclosure controls, let alone suggest that he sought for them to be designed unreasonably. And as to the internal accounting controls claim, the Complaint does not plausibly allege that Mr. Brown signed these sub-certifications because he knew and "wished to bring about" that SolarWinds had allegedly inadequate controls—which is an absurd notion to begin with given that Mr. Brown's job was to protect the Company's security.

CONCLUSION

The Amended Complaint should be dismissed in its entirety, with prejudice.

Dated: March 22, 2024

Respectfully submitted,

/s/ Serrin Turner

Serrin Turner
Nicolas Luongo
LATHAM & WATKINS LLP
1271 Avenue of the Americas

New York, NY 10020
Telephone: (212) 906-1200
Facsimile: (212) 751-4864
serrin.turner@lw.com
nicolas.luongo@lw.com

Sean M. Berkowitz (*pro hac vice*)
Kirsten C. Lee (*pro hac vice*)
LATHAM & WATKINS LLP
330 N. Wabash, Suite 2800
Chicago, IL 60611
Telephone: (312) 876-7700
Facsimile: (617) 993-9767
sean.berkowitz@lw.com
kirsten.lee@lw.com

Michael Clemente (*pro hac vice*)
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
Telephone: (202) 637-2200
Facsimile: (202) 637-2201
michael.clemente@lw.com

Counsel for Defendants SolarWinds Corp. and Timothy G. Brown

CERTIFICATE OF SERVICE

I hereby certify that on March 22, 2024, I electronically filed the foregoing document with the Court via CM/ECF, which will automatically send notice and a copy of same to counsel of record via email.

/s/ Serrin Turner
Serrin Turner